AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jared Jankowski, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Microsoft Corporation ("Microsoft"), an electronic communications service/remote computing service provider headquartered at 1 Microsoft Way, Redmond, WA 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account(s) identified in Attachment A, including the contents of communications.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been so employed since September 2017. I am currently assigned the FBI Pittsburgh Division, Charleston, West Virginia Resident Agency. In May 2018, I completed Special Agent training at the FBI training center in Quantico, Virginia. Upon graduation from the FBI academy, I was assigned to counterintelligence, where I worked multiple cases involving espionage against the United States. Following working

counterintelligence, I was assigned as the task force coordinator for the West Virginia Child Exploitation and Human Trafficking Task Force.

3. During my career, I gained experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks as well as the traits and characteristics of child pornography collectors and possessors and their use of computers or other electronic and media devices to facilitate the collection, possession, trading, distribution, access and receipt of child pornographic materials.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A have been committed by KONNOR W. LYONS. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY

7. This investigation concerns alleged violations of 18 U.S.C. §2252A(a) relating to material involving the sexual exploitation of minors.

d. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly transporting or shipping child pornography through the mail or in interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing child pornography using any means or facility of interstate or foreign commerce, or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. § 2252A(a)(5)(B) prohibits the knowing possession or access with intent to view child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting

interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

8. The following definitions apply to this Affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involves the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

c. "Child Sexual Abuse Material" ("CSAM") has the same meaning as "child pornography."

d. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).

e. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data

security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Mobile computing devices" are handheld electronic devices used for storing data (such as names, addresses, music, photographs, appointments, or notes) and utilizing computer programs. Some mobile computers also function as wireless communication devices and are used to access the Internet and send and receive e-mail. Mobile computers often include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media

include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Many users of these devices also use cloud storage applications to store data such as images and videos in order to back up data, duplicate data in order to access data from other devices, or to free up space on their device. Most mobile computers run computer software, giving them many of the same capabilities as personal computers. For example, mobile computer users can work with word-processing documents, spreadsheets, presentations, internet browsing and chat applications. Mobile computers may also include global positioning system ("GPS") technology for determining the location of the device. Mobile computing devices include, but are not limited to, laptops, tablets, and smartphones. This type of device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and a mobile computer. As the amount of data that people store on their mobile devices has increased, smartphones and other mobile computing devices are also commonly synched with, or connected to, a desktop or laptop computer for backup data storage. This allows users to access selected data, such as photos, emails, contacts, and documents, across multiple devices, or to recover this data if their mobile device is broken or lost.

j. A "wireless telephone" (or mobile telephone, cellular telephone, or smartphone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of

transmitters/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

k. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

l. "Minor" means any person under the age of 18 years. See 18 U.S.C. § 2256(1).

m. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means,

which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

n. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CDROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

9. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is possessed, produced, and distributed. Computers basically serve four functions in

connection with child pornography: production, communication, distribution, and storage.

a. Child pornographers can convert images into a computer-readable format with a scanner. With digital cameras, to include cellular telephones or tablets equipped with cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

b. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last decade. These drives can store hundreds of thousands of images at very high resolution. The same is true for mobile computing devices.

c. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Gmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as

well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, evidence of child pornography can be found on the user's computer in most cases.

d. As with most digital technology, communications made from a computer or mobile computing device are often saved or stored on that computer/device. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. Such information is often maintained indefinitely until overwritten by other data.

PEER TO PEER FILE-SHARING

10. Peer to Peer ("P2P") file-sharing allows individuals to meet each other through the Internet, engage in social networking, and trade files.

11. P2P file-sharing is a method of communication available to Internet users through the use of special computer software. Computers

are linked together through the Internet on this network, and using this software allows for the sharing of digital files between users on the network. A user first obtains the P2P computer software, which can be downloaded from the Internet. In general, P2P computer software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software.

12. One aspect of P2P file-sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time. The software utilized to download files from P2P networks will only download from a single source via a direct connection to that computer.

13. A P2P file transfer is assisted by reference to an IP address. This address, expressed as four sets of numbers separated by decimal points, is unique to the particular Internet connection being used by a particular computer during an online session. The IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers.

14. The computer running the file-sharing application, in this case a BitTorrent application, had an IP address assigned to it while it was connected to the Internet. BitTorrent users are able to see the IP address of any computer system that shares or receives files from them.

15. Third-party software is available to identify the IP address of the P2P computer sending a file. Such software monitors and logs Internet and local network traffic. The BitTorrent network can be

accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include: the BitTorrent client program; uTorrent client program; and Vuze client program, among others.

16. These client programs are publicly available and typically are free P2P client software programs that can be downloaded from the Internet.

17. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding."

18. Files or sets of files are shared on the BitTorrent network via the use of "Torrents." A "Torrent" is typically a small file that describes the file(s) to be shared. It is important to note that a "Torrent" does not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to complete a download. This information includes things such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent." The

"info hash" is a MD5 hash value of the set of data describing the file(s) referenced in the "Torrent." This set of data includes the MD5 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" on the BitTorrent network. The "Torrent" may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all the file(s) referenced in the "Torrent." "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent." There are many publicly available servers on the Internet that provide BitTorrent tracker services.

19. In order to locate "Torrents" of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include isohhunt.com and thepiratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrents" that describe the files they seek to download. Torrent indexing websites do not actually host the content (files) described by "Torrents," only the "Torrents" themselves. Once a "Torrent" is located on the website

that meets a user's keyword search criteria, the user will download the "Torrent" to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent." It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on MD5 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent," to include the remote peers/clients IP addresses.

20. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a Torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the Torrent indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent." Utilizing trackers and other BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing

the file or files. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact MD5 hash value of that piece which is described in the "Torrent." The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the "Torrent," will remain in that location until moved or deleted by the user.

21. Law enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. To search the network for these known torrents, law enforcement can quickly identify targets in their jurisdiction. Law enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info hash" MD5 hash values of Torrents. These Torrents being searched for are those that have been previously identified by law enforcement as being associated with such files.

22. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a

single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

23. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and downloading a file from. This information includes: 1) The suspect client's IP address; 2) A confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and 3) The BitTorrent network client program and version being utilized by the suspect computer. Third-party software available to law enforcement has the ability to log this information.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

24. On or about September 24, 2023, FBI Task Force Officer ("TFO") Daniel Miller ("TFO Miller"), a law enforcement officer assigned to the West Virginia Internet Crimes Against Children ("ICAC") Task Force and the FBI Violent Crimes Against Children ("VCAC") Task Force, initiated an Internet-based investigation to identify persons possessing and participating in the trafficking of child pornography using the BitTorrent P2P network.

25. During this investigation, investigators examined records from a law enforcement program used to monitor P2P downloads on BitTorrent and located an IP address associated with a computer believed to be in the vicinity of Huntington, West Virginia, that had been previously identified through investigative processes as containing digital media files believed to be child pornography. This IP address was identified as 73.251.204.170 (the "target IP address").

26. The program further indicated that the target IP address had been logged as possessing, via a P2P file sharing program, approximately 464 digital media files of suspected child pornography/child erotica on September 24, 2023, between the hours of 5:02 AM and 7:03 AM UTC (12:02 AM and 2:03 AM EST).

27. On or about September 2, 2024, TFO Miller again initiated an Internet-based investigation to identify persons possessing and participating in the trafficking of child pornography using the BitTorrent computer network using the same law enforcement program.

28. The program indicated that the target IP address had been logged as possessing, via a P2P file-sharing program, approximately 6 digital media files of suspected child pornography/child erotica on September 2, 2024, between the hours of 5:57 PM and 6:08 PM UTC (12:57 PM and 1:08 PM EST). Investigators downloaded those digital media files for review.

29. I reviewed the files downloaded from the target IP address on September 2, 2024, and determined, based upon my training and experience,

that several of these files depicted child pornography as defined by 18 U.S.C. § 2256(8). Three of these files are described below:

a. A photograph with filename "000404.jpg" depicted two nude prepubescent females with brown hair positioned on their hands and knees. The females' vaginas are fully exposed toward the camera. One female has a blue object penetrating her anus. The other female has a pink object penetrating her vagina.

b. A photograph with filename "000244.jpg" depicted a nude prepubescent female with blonde hair laying on a bed. The female's vagina is fully exposed, and her hands and legs are tied together with rope.

c. A photograph with filename "000076.jpg" depicted an adult male's erect penis. A clothed prepubescent female with brown hair is leaning over the adult male with his erect penis touching her mouth. The male had ejaculated into the child's mouth.

30. Investigators determined that the target IP address was issued to ISP Comcast Cable Communications, LLC ("Comcast").

31. On September 25, 2023, investigators served an administrative subpoena on Comcast seeking subscriber information for the customer who was assigned the target IP address on September 24, 2023. The subpoena response from Comcast identified the subscriber of the target IP address on September 24, 2023, as "Roger D. Lyons," with a service address of 3010 Chase Street, Huntington, WV 25704.

32. On October 21, 2024, investigators served an administrative subpoena on Comcast seeking subscriber information for the customer who was assigned the target IP address on September 2, 2024. The subpoena response from Comcast identified the subscriber of the target IP address on September 2, 2024, as "Roger D. Lyons," with a service address of 3010 Chase Street, Huntington, WV 25704.

33. During the course of the investigation, I learned that ROGER D. LYONS and his son, KONNOR W. LYONS, lived at 3010 Chase Street, Huntington, Wayne County, West Virginia 25704 since at least September 2023.

34. On November 1, 2024, United States Magistrate Judge Joseph K. Reeder signed an application for a residential search warrant for 3010 Chase Street, Huntington, Wayne County, West Virginia 25704.

35. On November 4, 2024, the search warrant was executed at the residence. Pursuant to the warrant, several electronic devices were seized. A preliminary review of the devices identified a OneDrive account associated with the email address konnorwolfelyons@outlook.com (the "TARGET ACCOUNT").

36. This preliminary review showed data files within the OneDrive account that, in my training and experience, I believe could be associated with CSAM. Specifically, the preliminary review revealed two data files in the OneDrive account named "Family Love Without Limits" and "Noche De Viernes Mama Con Tablet Papa Cogiendo E Hijo Dormido." According to FBI linguists, the Spanish title of the latter data file directly translates to "Friday night, mother with tablet, father

grabbing, and son asleep." However, FBI linguists stated that while the word "cogiendo" literally means grabbing, grasping, taking, catching, etc., in this context, it could be used as the vulgar slang word for "fucking."

37. KONNOR W. LYONS was interviewed by investigators while the search warrant was being conducted at his residence. In the interview, he admitted to viewing CSAM but stated that he deleted it after viewing.

38. On November 5, 2024, a Preservation Request for the information associated with the TARGET ACCOUNT was served upon Microsoft.

BACKGROUND CONCERNING MICROSOFT

39. Microsoft provides its users cloud-based accounts that allow users cloud access from internet-connected devices to send, receive, and store emails online. Microsoft accounts are typically identified by a single login, which typically derives from a subscriber's email address.

40. Based on my training and experience, I have knowledge that Microsoft allows subscribers to obtain accounts by registering on Microsoft via an email address. During the registration process, Microsoft may ask subscribers to create a username and password, and to provide basic personal information such as a name, an alternate email address for backup purposes, a telephone number, and in some cases a means of payment.

41. Thus, a subscriber's Microsoft account can be used to store email, other types of electronic communication, including instant messaging, photo and video sharing, voice calls, video chats, SMS text

messaging, and social networking, contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on cloud-based servers. Based on my training and experience, I have knowledge that evidence of who controlled, used, and/or created a Microsoft account may be found within such computer files and other information created or stored by the Microsoft subscriber. I also have knowledge that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

42. Based on my training and experience, I know that providers such as Microsoft also collect and maintain information about their subscribers, including information about their use of Microsoft services. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods use to connect to the account (such as logging into the account via a Microsoft login), and other log files that reflect usage of the account. Providers such as Microsoft also commonly have records of the IP address used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as Microsoft typically collect and maintain location data related to subscriber's use of Microsoft services, including data derived from IP addresses and/or GPS data.

43. Based on my training and experience, I have knowledge that providers such as Microsoft also collect information relating to the devices used to access a subscriber's account, such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by Microsoft in order to track what devices are using Microsoft's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I further submit that such identifiers may constitute evidence of the offense under investigation because they can be used (a) to find other Microsoft accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the Microsoft account.

44. Based on my training and experience, I have knowledge that providers such as Microsoft use cookies and similar technologies to track users web history through use of cookies. Basically, a "cookie" is a small file containing a string of characters that a website attempts to

place onto a user's device. When that device visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to Microsoft. More sophisticated cookie technology can be used to identify users across devices and web browsers. From my training and experience, I have knowledge that cookies and similar technology used by providers such as Microsoft may constitute evidence of the offense under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a Microsoft account and determine the scope of criminal activity.

45. Based on my training and experience, I have knowledge that Microsoft may maintain records that can link different Microsoft accounts to one another, by virtue of common identifiers, such as common email addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Microsoft accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Microsoft account.

46. Based on my training and experience, I have knowledge that subscribers can communicate directly with Microsoft about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Microsoft typically

retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by Microsoft or the user as a result of the communications. I further submit that such information may constitute evidence of the offense under investigation because the information can be used to identify the account's user or users.

47. In summary, based on my training and experience in this context, I believe that the computers of Microsoft are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved email for Microsoft subscribers), as well as Microsoft-generated information about its subscribers and their use of Microsoft serves and other online services. In my training and experience, all of that information may constitute evidence of the offense under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide Microsoft with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

48. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information

described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

49. Based on the foregoing, I request that the Court issue the proposed search warrant.

50. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft. Because the warrant will be served on Microsoft, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Further your affiant sayeth not.

JARED JANKOWSKI
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Signed and sworn to by telephonic means on this 2nd day of December, 2024.

JOSEPH K. REEDER
UNITED STATES MAGISTRATE JUDGE